

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 09212365
PUBLICATION DATE : 15-08-97

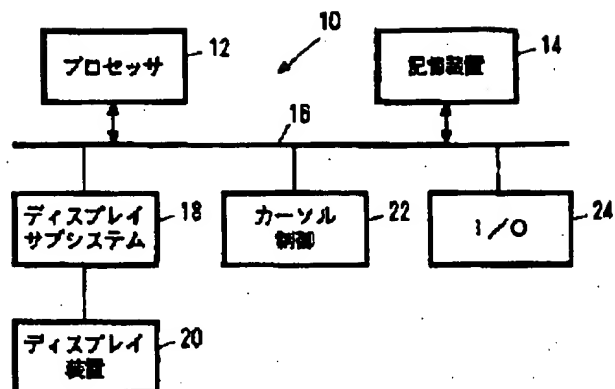
APPLICATION DATE : 25-12-96
APPLICATION NUMBER : 08345679

APPLICANT : INTERNATL BUSINESS MACH CORP
<IBM>;

INVENTOR : NADALIN ANTHONY J;

INT.CL. : G06F 9/44 G06F 12/14

TITLE : SYSTEM, METHOD, AND PRODUCT
FOR INFORMATION HANDLING
INCLUDING INTEGRATION OF
OBJECT SECURITY SERVICE
APPROVAL IN DECENTRALIZED
COMPUTING ENVIRONMENT



ABSTRACT : PROBLEM TO BE SOLVED: To integrate object security service approvals in a decentralized computing environment by allocating and selecting a set of method request access rights.

SOLUTION: The information handling system 10 is equipped with a processor 12, a storage device 14, a system bus 16, a display subsystem 18 which controls a display device 20, a cursor controller 22, and an I/O controller 24. An object-oriented control program maps a set of methods defined in a given class to a set of fixed finite access rights to which a set of method request access rights is assigned. And, a set of permissions regarding a 1st and a 2nd family right type permissions is inspected to select a set of access rights.

COPYRIGHT: (C)1997,JPO

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-212365

(43)公開日 平成9年(1997)8月15日

| (51)Int.Cl. ⁶ | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
|--------------------------|-------|--------|--------------|---------|
| G 0 6 F 9/44 | 5 3 0 | | G 0 6 F 9/44 | 5 3 0 C |
| 12/14 | 3 1 0 | | 12/14 | 3 1 0 K |

審査請求 未請求 請求項の数14 O L (全 7 頁)

(21)出願番号 特願平8-345679

(22)出願日 平成8年(1996)12月25日

(31)優先権主張番号 08/582550

(32)優先日 1996年1月3日

(33)優先権主張国 米国 (US)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州
アーモンク (番地なし)

(72)発明者 メサウド・ペナンタール

アメリカ合衆国12603、 ニューヨーク州
ボウキプスイ ジャックマン ドライブ
エス 39-ビー

(74)代理人 弁理士 合田 潔 (外2名)

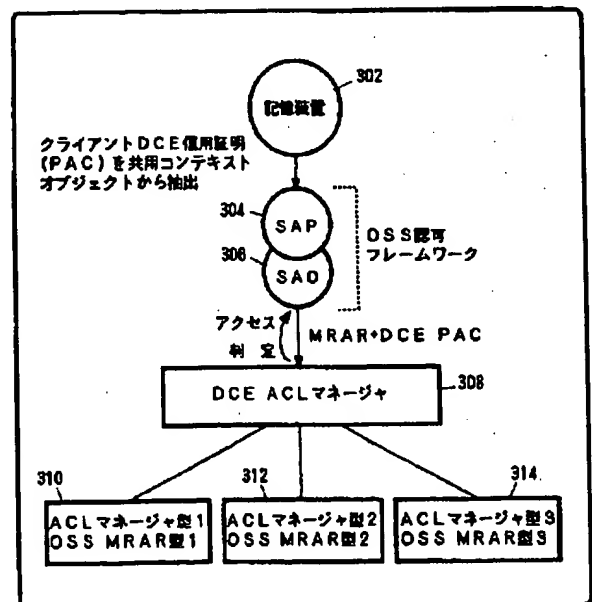
最終頁に続く

(54)【発明の名称】 分散コンピューティング環境でのオブジェクト・セキュリティ・サービス認可の統合を含む情報取り扱いシステム、方法および製品

(57)【要約】

【課題】分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合する。

【解決手段】オブジェクト指向制御プログラムが、所与のクラスによって定義されるメソッドのセットを、メソッド要求アクセス権のセットが割り当てられる固定された有限のアクセス権のセットに対してマッピングすることと、二つの要素、すなわち第一のファミリー権利型(権利型とは、その許可のセットの意味規則を指図する要素である)および第二の、そのようなファミリーそれぞれに関する許可のセットを検査することによってアクセス権のセットを選択することを含む。二つのファミリー型、すなわちオペレーション権利および役割権利を用いることができる。本発明の実施態様のスケーリング性は、新たな権利型のファミリーを、ファミリーごとに対応する許可のセットとともに追加する能力によって実証することができる。



【特許請求の範囲】

【請求項1】第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするステップと、
メソッド要求アクセス権のセットを割り当てるステップと、

前記アクセス権のセットを選択するステップと、を含むことを特徴とする、情報取り扱いシステムにおいてオブジェクト指向技術を用いる方法。

【請求項2】前記方法がステップが、
前記アクセス権のセットの二つの要素を検査するステップをさらに含む請求項1記載の方法。

【請求項3】前記二つの要素の第一のものがファミリー権利型である請求項1記載の方法。

【請求項4】前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである請求項1記載の方法。

【請求項5】ファミリー権利型が、
オペレーション権利と、
役割権利と、を含む請求項3記載の方法。

【請求項6】第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、
メソッド要求アクセス権のセットを割り当てるための手段と、
前記アクセス権のセットを選択するための手段と、をさらに含むコンピュータ読み出し可能媒体。

【請求項7】前記媒体が、前記アクセス権のセットの二つの要素を検査するための手段をさらに含む請求項6記載のコンピュータ読み出し可能媒体。

【請求項8】前記二つの要素の第一のものがファミリー権利型であり、
前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである請求項5記載のコンピュータ読み出し可能媒体。

【請求項9】1個以上のプロセッサと、
記憶装置と、
ディスプレイ装置を制御するディスプレイ・サブシステムと、
カーソル制御装置と、
1個以上のI/O装置を制御する1個以上のI/O制御装置と、
前記プロセッサ、前記記憶装置、前記ディスプレイ・サブシステム、前記カーソル制御装置および前記I/O制御装置を接続するシステム・バスと、
システムの動作を制御するためのオペレーティング・システム・プログラムと、
ユーザ・タスクを実行するための一つ以上のアプリケーション・プログラムと、
オブジェクト指向制御プログラムと、を含み、

前記オブジェクト指向制御プログラムが、
第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、
メソッド要求アクセス権のセットを割り当てるための手段と、

前記アクセス権のセットを選択するための手段と、を含むことを特徴とする、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合するための情報取り扱いシステム。

【請求項10】前記アクセス権のセットの二つの要素を検査するための手段をさらに含む請求項9記載の情報取り扱いシステム。

【請求項11】前記二つの要素の第一のものがファミリー権利型である請求項10記載の情報取り扱いシステム。

【請求項12】前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである請求項10記載の情報取り扱いシステム。

【請求項13】前記ファミリー権利型が、関連する許可のセットの意味規則を制御する要素である請求項11記載の情報取り扱いシステム。

【請求項14】ファミリー権利型が、
オペレーション権利と、
役割権利と、を含む請求項10記載の情報取り扱いシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報取り扱いシステム、方法および製品に関し、より詳細には、オブジェクト指向システムにおいてオブジェクト・セキュリティを高めるための情報取り扱いシステム、方法および製品に関する。

【0002】

【従来の技術】オブジェクト指向システムにおいてはセキュリティを改善する必要がある。従来から、リソースへのアクセスを制御することは、データを開示したり、変更したり、更新したりすることができるかどうかを決定することを意味する。しかし、オブジェクト指向システムにおけるアクセス制御は、異なるアспектおよび意味規則を呈する。オブジェクト指向システムにおいては、リソースは、データのみからなるオブジェクトではなく、オブジェクトのデータを改ざん、変形することができる操作をも含むオブジェクトである。そのようなものとして、オブジェクト・アクセス制御は、どのユーザがどのオブジェクトに対してどのメソッドを呼び出すことができるかの決定に関する。したがって、アクセス権が、それが当てはまるメソッドの機能性および副作用の意味規則に対応しなければならない。もっとも簡単な場合、この対応は1対1であることができる。すなわち、

メソッドMの必要なアクセス権は、そのメソッドの名称、すなわち単にMによってそれを定義するクラスにおいて一意的に識別することができる。したがって、主体は、メソッドMを呼び出し、その副作用を期待するためには、許可Mを取得しなければならないであろう。しかし、オブジェクト指向システムは、それぞれ異なるシグナチャおよび意味規則をもつ非常に多数のタイプのオペレーション（メソッド）を露呈する傾向にあるため、この方法は、スケールの問題を招く。アプリケーションの保護されたオブジェクトに対するこのようなアクセス制御は、アクセス権または許可の意味規則が一般に手近にあるアプリケーションだけに有効であるということにおいて、その特定のアプリケーションに適合させなければならない。加えて、クラス・ライブラリが新たに導入されるごとにアクセス権または許可のセットがサイズを急速に増すため、オブジェクト・アクセス制御の管理は複雑なタスクになる。

【0003】従来技術において、オブジェクト指向プログラミング・システム（OOPS）を改善するための技術が数多くある。

【0004】以下に従来技術の例を示す。

【0005】米国特許第4,525,780号明細書は、オブジェクトに編成されたメモリを有するデータ処理システムであって、システムが、ユーザを識別する主体番号、ユーザの手続きを実行するためのプロセスおよびユーザの手続きによって実行されるシステム・オペレーションのタイプによって識別されるユーザによるオブジェクトに対する無許可のアクセスを防止する保護技術を利用するシステムを教示している。

【0006】米国特許第5,136,712号明細書は、オブジェクトをプロセスに対して私用にするための手段を含む、マルチタスク処理コンピュータ・システムに用いるためのオブジェクトベースのオペレーティング・システムを教示している。私用オブジェクトに対するアクセスは、アクセス制御リストによって制御される。

【0007】米国特許第5,265,221号明細書は、動詞、パラメータ、属性および機能のシステムを使用して、オブジェクトに対する認可を付与し、取り消し、否定するためのアクセス制御機構を教示している。

【0008】米国特許第5,297,283号明細書および米国特許第5,321,841号明細書は、上記に論じた米国特許第5,136,712号明細書と同じシステムを教示していると思われる。

【0009】米国特許第5,093,914号明細書は、概して、オブジェクト指向プログラムの実行の制御において、定義された動作を実施する、例えば、プログラムの実行中に指定のオブジェクトに対して指定の仮想機能が呼びされたときにプログラムを停止するために、デジタル・コンピュータによって使用される方法を教示している。

【0010】米国特許第5,343,554号明細書は、第二のクラス・オブジェクトが外部的に呼び出し可能であり、外部的に呼び出し可能であるサブクラス・オブジェクトが内部的に呼び出し可能なサブクラス・オブジェクトの指示を含むような第一および第二のクラスのオブジェクトを作成することと、一つの外部的に呼び出し可能なサブオブジェクトが内部的に呼び出し可能なサブオブジェクトを呼び出し、その結果に応じて第一のクラスの新たなオブジェクトが生成されるようなオブジェクトのクラスを実行することとを含むプロセスによって問題が解決されるコンピューティング・システムを教示している。

【0011】これらの特許は、一般に、オブジェクト指向プログラムにおいてオブジェクトをアクセスから保護する方法を扱うが、これらは、本明細書の特許請求の範囲の記載の開示するような、メソッド要求アクセス権のセットを割り当て、選択することによってスケールの問題を解決することを教示してもいいし示唆してもいい。

【0012】オブジェクト・サービス機能、例えば持続性、回復性、並行性およびセキュリティを自動的に2進（バイナリ）クラスに追加する必要がある。ときには、クラスのソース・コードを変更できないこともある。ソース・コードを変更することができる場合でさえ、オブジェクト・サービス機能を追加するためには相当な再プログラムの努力を要する。

【0013】

【発明が解決しようとする課題】本発明の目的は、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合することにある。

【0014】

【課題を解決するための手段】したがって、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合するためのシステム、方法および製品は、1個以上のプロセッサと、記憶装置と、システム・バスと、ディスプレイ装置を制御するディスプレイ・サブシステムと、カーソル制御装置と、I/O装置を制御するI/O制御装置と（すべてシステム・バスによって接続）、オペレーティング・システム、例えばOS/2オペレーティング・システム・プログラム（OS/2はInternational Business Machines社の登録商標である）と、ユーザ・タスクを実行するための一つ以上のアプリケーション・プログラムと、オブジェクト指向制御プログラム、例えば、International Business Machine社の市販品であるDSOMオブジェクト・プログラムとを含み、前記オブジェクト指向制御プログラムが、所与のクラスによって定義されるメソッドのセットを、メソッド要求アクセス権のセットが割り当てられる固定された有限のアクセス権のセットに対してマッピングすることと、二つの要素、すなわち第一のファミリー権利型

(権利型とは、その許可のセットの意味規則を指図する要素である)および第二の、そのようなファミリーそれぞれに関する許可のセットを検査することによってアクセス権のセットを選択することを含む。二つのファミリー型、すなわちオペレーション権利および役割権利を用いることができる。本発明の実施態様のスケーラビリティ(拡張性)は、新たな権利型のファミリーを、ファミリーごとに対応する許可のセットとともに追加する能力によって実証することができる。

【0015】本発明の利点は、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合することにより、分散オブジェクト・システムにおけるオブジェクト・セキュリティが改善されることにある。

【0016】

【発明の実施の形態】まず、図1および2を参照しながら、本発明の情報取り扱いシステム10およびオペレーティング・システム環境を説明する。

【0017】情報取り扱いシステム10は、1個以上のプロセッサ12、記憶装置14、システム・バス16、ディスプレイ装置20を制御するディスプレイ・サブシステム18、カーソル制御装置22およびI/O制御装置24(すべてシステム・バス16によって接続)を備えたグラフィックス・ワークステーションなどであることができる。図1に示す情報取り扱いシステム10は、市販されている周知のマルチタスク処理オペレーティング・システム、例えばOS/2(OS/2はInternational Business Machines社の登録商標である)によって動作することができる。情報取り扱いシステム10を動作させる際にOS/2オペレーティング・システムが制御する多数のタスクの中には、オブジェクト指向プログラム、例えば、International Business Machines社の市販品であるDSOMオブジェクト・プログラムの実行がある。

【0018】本発明の方法は、DSOMオブジェクト・プログラムに組み入れることができる。

【0019】2進クラスのオブジェクトのアクセス制御はオブジェクト保証(Secure object)サービスによって提供される。このオブジェクト保証サービスを説明する。

【0020】ユーザがセキュリティを指定する方法は、クラス・オブジェクトを探索するときに、以下の制約を指定することである。

【0021】名称:保証

値:オブジェクトがアクセス制御検査によって保護され

るかどうかを示す論理フラグ

名称:ACL

値:保証=真ならば、アクセス制御リスト

【0022】実現方法がメソッドによるとき、メソッドの呼び出しに応じて実施することができるか、参照が最初に得られたときに実施することができるかのいずれかである(ケイパビリティ方式)。ケイパビリティ(資格)方式は、オブジェクトと、許可されたメソッドのサブセットだけを有するACL(許可されたメソッドのリスト)との組み合わせごとにセキュリティ代理(proxy)オブジェクトをサーバ中に構築することによって実施することができる。これを実施するためには、ORB(または少なくともサーバ・オブジェクト)を変更しなければならないであろう。

【0023】リソースに対するアクセスを制御する際には、アクセス権または許可のセットが、それらが当てはまるメソッドの意味規則に対応しなければならない。新たなクラス・ライブラリが導入されるごとにアクセス権または許可のセットがサイズを増すため、オブジェクト・アクセス制御の管理は複雑なタスクになる。スケーリング性を扱うためには、所与のクラスによって定義されるメソッドのセットを、メソッド要求アクセス権のセット(MRAR)が割り当てられる固定された有限のアクセス権のセットに対してマッピングする。そして、問題は、適当なアクセス権のセットを選択するということになる。セットを二つの要素、すなわち、ファミリー権利型と、そのようなファミリーそれぞれに関する許可のセットとに分割することにより、多数のアクセス権または許可のセットを有するシステムにおいてさえ、アクセス制御を効率的に扱うことができる。

【0024】本発明の好ましい実施態様においては、二つの標準的なファミリー型、すなわちオペレーション権利および役割権利を述べる。スケーリング性の課題は、システムが新たな権利型のファミリーを、そのようなファミリーごとに対応する許可のセットとともに追加する能力によって取り扱われる。好ましくは標準タイプのオペレーション型および役割型に限定された少数のファミリー権利型を各ファミリー内の固定された少数の許可のセットとともに維持するならば、アクセス制御および移植性が高まる。

【0025】以下の表1は、二つの標準的な権利型とその関連の権利および解釈とともに示す。

【0026】

【表1】

権利型
OPERATION_RIGHTS

表1
権利型
権 利
R
W

意図する解釈
読み
書き

ROLE_RIGHTS

X
C
D
A
G
U
O
M
T
S実行
制御
削除
追加
ゲスト
ユーザ
オペレータ
管理者
監査者
監督者

【0027】次に図3を参照しながら、本発明と、分散コンピューティング環境の認可機構との統合を説明する。セキュリティ記憶装置(vault)302がオブジェクト・セキュリティ・サービスの基本要素である。認可信用証明(credential)がオブジェクトごとに記憶装置302中に記憶されている。クライアントのDCE信用証明が共有コンテキスト・オブジェクトから抽出され、システム認可方針オブジェクト304に提示され、このシステム認可方針オブジェクトが、システム認可オラクル(oracle)306と合わさって、事前に確立した認可方針に基づき、認可の判定を下す。認可の判定は、システム認可オラクル306からDCE ACLマネージャ308に送られる。メソッドのMRAR権利型は、DCE ACLマネージャの型、例えばACLマネージャ型1およびMRAR型1(310)、ACLマネージャ型2、MRAR型2(312)またはACLマネージャ型3、MRAR型3(314)に対応する。DCEマネージャ型310、312、314は、以下のDCE API

sec_acl_mgr_types_semantics

によって検索することができ、これが、所与のオブジェクトを保護するACLに対応するマネージャ型のセットを戻す。そして、認可検査の過程で、メソッドのMRARの意味規則に対応するDCE ACLが適用される。メソッドのMRARをビットマップ列にマッピングすることにより、速やかな認可検査が実行される。

【0028】二つのアクセス意味規則を区別することができる。

【0029】1. 認可検査がうまく行くためには全MRARセットのAND条件が満たされなければならない。これは、全MRARビットマップを、以下のDCE認可API

sec_acl_test_access_on_behalf

のための所望のアクセスとしてセットすることに対応する。

【0030】2. MRARセットの一つの権利だけというOR条件が満たされる必要がある。この場合、ビットマップ所望アクセス・フラグが一度に1ビットをとり、判定に遭遇するまでMRARセットをスパンする。そして、アクセスに失敗すると、全MRARセットをスパン

しなければならないが、第一のMRAR許可がアクセスを許可すると、認可ルーチンが正常な認可の結果を戻す。

【0031】まとめとして、本発明の構成に関して以下の事項を開示する。

(1) 第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするステップと、メソッド要求アクセス権のセットを割り当てるステップと、前記アクセス権のセットを選択するステップと、を含むことを特徴とする、情報取り扱いシステムにおいてオブジェクト指向技術を用いる方法。

(2) 前記方法がステップが、前記アクセス権のセットの二つの要素を検査するステップをさらに含む上記

(1) 記載の方法。

(3) 前記二つの要素の第一のものがファミリー権利型である上記(1)記載の方法。

(4) 前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである上記(1)記載の方法。

(5) ファミリー権利型が、オペレーション権利と、役割権利と、を含む上記(3)記載の方法。

(6) 第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、メソッド要求アクセス権のセットを割り当てるための手段と、前記アクセス権のセットを選択するための手段と、をさらに含むコンピュータ読み出し可能媒体。

(7) 前記媒体が、前記アクセス権のセットの二つの要素を検査するための手段をさらに含む上記(6)記載のコンピュータ読み出し可能媒体。

(8) 前記二つの要素の第一のものがファミリー権利型であり、前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである上記(5)記載のコンピュータ読み出し可能媒体。

(9) 1個以上のプロセッサと、記憶装置と、ディスプレイ装置を制御するディスプレイ・サブシステムと、カーソル制御装置と、1個以上のI/O装置を制御する1個以上のI/O制御装置と、前記プロセッサ、前記記憶装置、前記ディスプレイ・サブシステム、前記カーソル制御装置および前記I/O制御装置を接続するシステム・バスと、システムの動作を制御するためのオペレーテ

ィング・システム・プログラムと、ユーザ・タスクを実行するための一つ以上のアプリケーション・プログラムと、オブジェクト指向制御プログラムと、を含み、前記オブジェクト指向制御プログラムが、第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、メソッド要求アクセス権のセットを割り当てるための手段と、前記アクセス権のセットを選択するための手段と、を含むことを特徴とする、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合するための情報取り扱いシステム。

(10) 前記アクセス権のセットの二つの要素を検査するための手段をさらに含む上記(9)記載の情報取り扱いシステム。

(11) 前記二つの要素の第一のものがファミリー権利型である上記(10)記載の情報取り扱いシステム。

(12) 前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである上記(10)記載の情報取り扱いシステム。

(13) 前記ファミリー権利型が、関連する許可のセットの意味規則を制御する要素である上記(11)記載の情報取り扱いシステム。

(14) ファミリー権利型が、オペレーション権利と、役割権利と、を含む上記(10)記載の情報取り扱いシステム。

【図面の簡単な説明】

【図1】本発明を具現化するシステムのブロック図である。

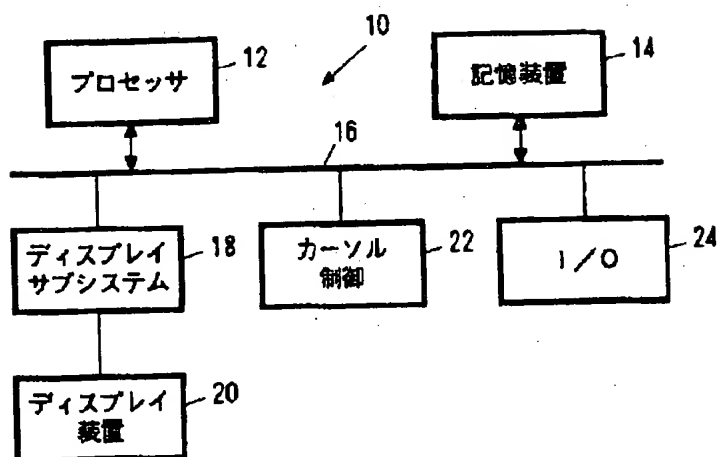
【図2】本発明を支援するオペレーティング・システム・プラットフォームおよびシステム・オブジェクト・モデル・プログラムを示すブロック図である。

【図3】本発明を具現化する分散オブジェクト・システムの略図である。

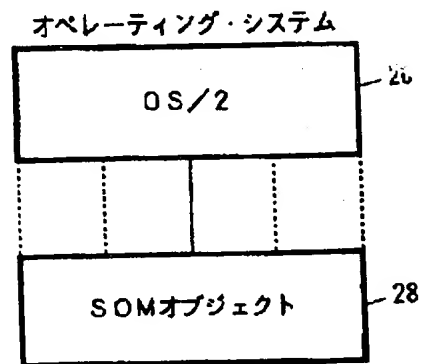
【符号の説明】

- 10 情報取り扱いシステム
- 12 プロセッサ
- 14 記憶装置
- 16 システム・バス
- 18 ディスプレイ・サブシステム
- 20 ディスプレイ装置
- 22 カーソル制御装置
- 24 I/O制御装置
- 302 セキュリティ記憶装置
- 304 システム認可方針オブジェクト
- 306 システム認可オラクル
- 308 DCE ACLマネージャ
- 310 ACLマネージャ型1、MRAR型1
- 312 ACLマネージャ型2、MRAR型2
- 314 ACLマネージャ型3、MRAR型3

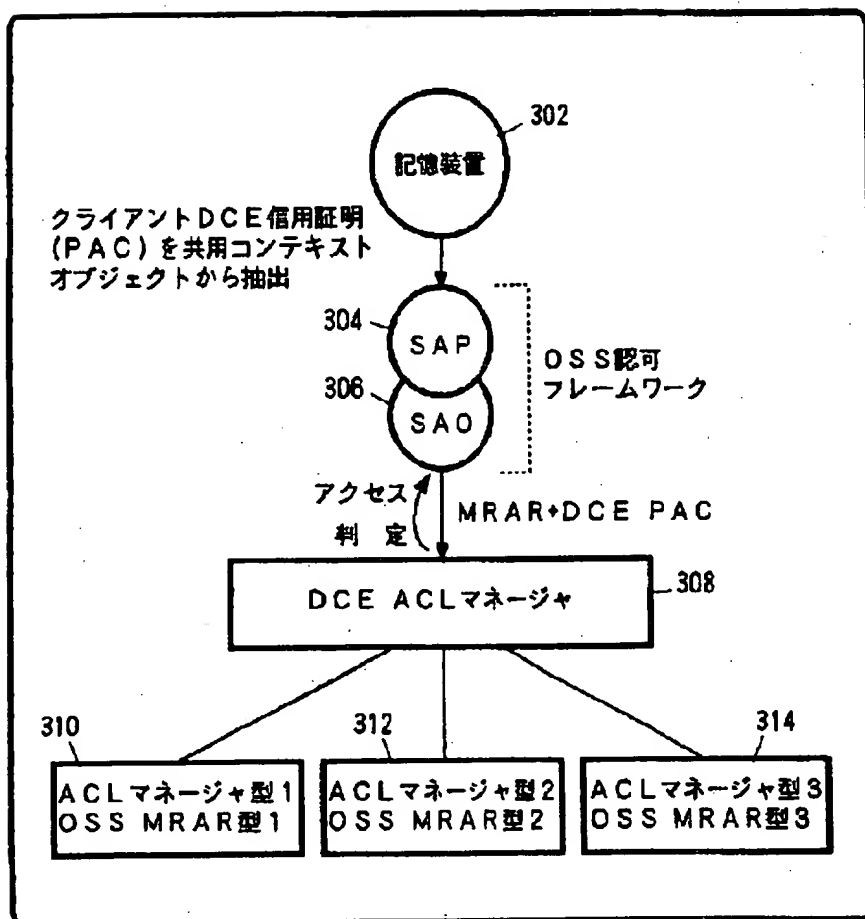
【図1】



【図2】



【図3】



フロントページの続き

(72)発明者 ジョージ・ロバート・ブラクリィ・サード
アメリカ合衆国78729、 テキサス州オー
スティン スティルフォレスト 13007

(72)発明者 アンソニー・ジョセフ・ナダリン
アメリカ合衆国78759、 テキサス州オー
スティン デュヴァル・ロード 3201 ア
パートメント 623

THIS PAGE BLANK (USPTO)